PUBLIC-KEY CRYPTOGRAPHIC SCHEMES SECURE AGAINST AN ADAPTIVE CHOSEN CIPHERTEXT ATTACK IN THE STANDARD MODEL

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention relates to a public-key cryptographic scheme and cryptographic communications using public-key cryptography.

DESCRIPTION OF THE RELATED ART

Various types of public-key cryptographic schemes have been proposed to date. Of these schemes, the most famous and most practical public-key cryptographic scheme is described in:

a document 1: "R. L. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, Vol. 21, No. 2, pp. 120-126, 1978".

Efficient public-key cryptographic schemes using elliptic curves are known as described in:

a document 2: "V. S. Miller: Use of Elliptic Curves in Cryptography, Proc. of Crypto'85, LNCS218, Sprinter-Verlag, pp. 417-426 (1985);

a document 3: "N. Koblitz: Elliptic Curve Cryptosystems, Math. Comp., 48, 177, pp. 203-209 (1987)"; and the like.

Known cryptographic schemes capable of

verifying security against chosen plaintext attacks include:

a document 4: "M. O. Rabin: Digital Signatures and Public-Key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCS/TR-212 (1979)";

a document 5: "T. ElGamal: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. On Information Theory, IT-31, 4, pp. 469-472 (1985)";

a document 6: "S. Goldwasser and S. Micali: Probabilistic Encryption, JCSS, 28, 2, pp. 270-299 (1984);

a document 7: "M. Blum and S. Goldwasser: An Efficient probabilistic public-key encryption scheme which hides all partial information, Proc. of Crypto'84, LNCS196, Springer-Verlag, pp. 289-299 (1985)";

a document 8: S. Goldwasser and M. Bellare: Lecture Notes on Cryptography, http://www-cse.ucsd.edu/users/mihir/ (1997)"; and

a document 9: "T. Okamoto and S. Uchiyama: A new Public-Key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt'98, LNCS1403, Springer-Verlag, pp. 308-318 (1998)".

Known cryptographic schemes capable of verifying security against chosen ciphertext attacks include:

a document 10: "D. Dolve, C. Dwork and M. Naor: Non-malleable cryptography, In 23rd Annual ACM Symposium on Theory of Computing, pp. 542-552 (1991)";

a document 11: "M. Naor and M. Yung: Public-key cryptosystems probably secure against chosen ciphertext attacks, Proc. of STOC, ACM Press, pp. 427-437 (1990)";

a document 12: "M. Bellare and P. Rogaway: Optimal Asymmetric Encryption How to Encrypt with RSA, Proc. of Eurocrypt'94, LNCS950, Springer-verlag, pp. 92-111 (1994)"; and

a document 13: "R. Cramer and V. Shoup: A practical PUblic Key Cryptosystem Probably Secure against Adaptive Chosen Ciphertext Attack, Proc. of Crypto'98, LNCS1462, Springer-Verlag, pp. 13-25 (1998)".

A document 14: "M. Bellare, A. Desai, D. Pointcheval and P. Rogaway: Relations Among Notions of Security for Public-Key Encryption Schemes, Proc. of Crypto'98, LNSC1462, Sprinter-Verlag, pp. 26-45 (1998)", indicates the equivalency between IND-CCA2 (semantically secure (indistinguishable) against adaptive chosen ciphertext attacks) and NM-CCA2 (non-malleable against adaptive chosen ciphertext attacks). A public-key cryptographic scheme satisfying this condition is presently considered most secure.

Although the public-key cryptographic scheme described in the document 12 is practical, security is verified on the assumption that an ideal random function exists. Since it is impossible to configure an ideal random function in a real system, the ideal random function is replaced with a practical hash function in order to apply the scheme of the document 12 to the real system. Therefore, security cannot be verified in the real system.

The document 13 provides a public-key cryptographic scheme capable of verifying IND-CCA2 on the assumption that a general one-way hash function exists instead of an ideal random function. Since the general one-way hash function can be configured really (under a cryptographic assumption), the scheme described in the document 13 can verify security in a standard model. However, when it is applied to a real system, a practical hash function such as SHA-1 is used by assuming it as a general hash function in order to improve the efficiency. Therefore, a strong assumption is incorporated in order to verify security. Although the document 13 proposes a public-key cryptographic scheme which does not assume the existence of a general one-way hash function, the efficiency of this scheme is inferior to a scheme which assumes the existence of a general one-way hash function.

SUMMARY OF THE INVENTION

It is a main object of the present invention to provide a public-key cryptographic scheme which is practical and capable of verifying security (IND-CCA2) against strongest attacks or adaptive chosen ciphertext attacks in a standard model (a real computer model not assuming the existence of an ideal function).

It is another object of the present invention to provide a public-key cryptographic scheme which is practical and capable of verifying security even if it is applied to a real system, by assuming only the difficulty of the Diffe-Hellman decision problem.

It is another object of the invention to provide a cryptographic communication method using the public-key cryptographic scheme of the invention, a program, an apparatus and a system for executing the method.

In order to achieve the above objects of the invention, a ciphertext is created by using a combination of a plaintext and random numbers in order to reject an illegal ciphertext input to a (simulated) deciphering oracle and to guarantee security against adaptive chosen ciphertext attacks. The environment given a deciphering oracle means an environment which unconditionally gives the deciphered results of any ciphertext excepting a target ciphertext. According to one of specific public-key cryptographic schemes, the following secret-key is created:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and the following public key is created:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = {g_1}^{x_1}{g_2}^{x_2} \bmod p,\ d_1 = {g_1}^{y_{11}}{g_2}^{y_{12}} \bmod p,\ d_2 = {g_1}^{y_{21}}{g_2}^{y_{22}} \bmod p,\ h = {g_1}^{z} \bmod p,$
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$

(ord() indicates an order)

A sender generates a random number $\alpha = \alpha_1 \| \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for a plaintext m ($|m| = k_3$ where $|x|$ indicates the number of digits of x), and calculates:

$$\tilde{m} = \alpha \| m$$

A random number $r \in Zq$ is selected, and the following is calculated:

$$u_1 = {g_1}^{r} \bmod p, \quad u_2 = {g_2}^{r} \bmod p, \quad e = \tilde{m}\, h^{r} \bmod p, \quad v = {g_1}^{\alpha_1} c^{r} {d_1}^{\alpha r} {d_2}^{mr} \bmod p$$

A ciphertext (u_1, u_2, e, v) is transmitted to a receiver.

By using a secret-key of the receiver and the received ciphertext, the receiver calculates α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$), and $|m'| = k_3$ which satisfy:

$$\alpha'_1 \| \alpha'_2 \| m' = e / {u_1}^{z} \bmod p$$

If the following is satisfied;

$${g_1}^{\alpha'_1} {u_1}^{x_1 + \alpha' y_{11} + m' y_{21}} {u_2}^{x_2 + \alpha' y_{12} + m' y_{22}} \equiv v \pmod{p}$$

m' is output as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$), whereas if not satisfied, the effect that the received ciphertext is rejected is output as the decipher results.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagram showing the structure of a system according to an embodiment of the invention.

Fig. 2 is a diagram showing the internal structure of a sender side apparatus of the embodiment.

Fig. 3 is a diagram showing the internal structure of a receiver side apparatus of the embodiment.

Fig. 4 is a diagram showing the outline of a second embodiment of the invention.

Fig. 5 is a diagram showing the outline of a fourth embodiment of the invention.

Fig. 6 is a diagram showing the outline of a sixth embodiment of the invention.

DETAILED DESCRIPTION OF THE EMBODIMENTS

Embodiments of the invention will be described with reference to the accompanying drawings.

Fig. 1 is a diagram showing the structure of a system according to an embodiment of the invention. This system is constituted of a sender side apparatus 100 and a receiver side apparatus 200. The sender side apparatus 100 and receiver side apparatus 200 are connected by a communication line 300.

Fig. 2 is a diagram showing the internal structure of the sender side apparatus 100 of the embodiment. The sender side apparatus 100 has a random number generator unit 101, an exponentiation unit 102, a calculation unit 103, a modular calculation unit 104, a memory unit 105, a communication unit 106, an input unit 107 and an encipher unit 108. A plaintext m to be enciphered is input from the input unit 107, created on the sender side apparatus 100, or supplied from the communication unit 106 or an unrepresented storage unit.

Fig. 3 is a diagram showing the internal structure of the receiver side apparatus 200 of the embodiment. The receiver side apparatus 200 has a key generator unit 201, an exponentiation unit 202, a modular calculation unit 203, a calculation unit 204, a memory unit 205, a communication unit 206 and a decipher unit 207. Although not shown, the receiver side apparatus has an output unit for supplying the user (receiver) of the apparatus with the deciphered results by means of display, sounds and the like.

The sender side apparatus 100 and receiver side apparatus 200 may be a computer having a CPU and a memory.

The random number generator unit 101, exponentiation units 102 and 202, modular calculation units 104 and 204, key generator unit 201, encipher unit 108 and decipher unit 207 each may be a custom processor matching the length of bits to be processed, or may be realized by software programs running on a central processing unit (CPU).

Processes for key generation, encipher/decipher and ciphertext transmission/reception to be described in the following embodiments are realized by software programs running on the CPU. The software programs use the above-mentioned units.

Each software program is stored in a computer readable storage medium such as a portable storage medium and a communication medium on the communication line.

I First Embodiment

This embodiment describes a public-key cryptographic scheme.

1. Key Generating Process

In response to an operation by a receiver B, the key generator unit 201 of the reception side apparatus 200 generates beforehand secret information constituted of seven numbers:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and public information:

- G, G' : finite (multiplicative) group $\quad G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2},\ d_1 = g_1^{y_{11}} g_2^{y_{12}},\ d_2 = g_1^{y_{21}} g_2^{y_{22}},\ h = g_1^{z},$
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1,\ \forall \alpha_2 \in X_2)$$

M is a plaintext space, and || represents a concatenation of bit trains. The public information is supplied to the sender side apparatus 100 or made public, via the communication line 300 or the like. A publicizing method may be registration in the third party (public information management facilities) or may be a well-known method. Other information is stored in the memory unit 205.

2. Encipher/Decipher Process

(1) In response to an operation by a sender A, the random number generator unit 101 of the sender side apparatus 100 selects random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Zq$ for the plaintext m ($m \in M$), and the exponentiation unit 102, calculation unit 103 and modular calculation unit 104 calculate:

$$u_1 = g_1^{r}, \quad u_2 = g_2^{r}, \quad e = \pi(\alpha_1, \alpha_2, m) h^{r}, \quad v = g_1^{\alpha_1} c^{r} d_1^{\alpha r} d_2^{mr}$$

where $\alpha = \alpha_1 \mid\mid \alpha_2$. In response to an operation by the sender A, the communication apparatus 106 of the sender side apparatus 100 transmits the ciphertext (u_1, u_2, e, v) to the receiver side apparatus 200 via the communication line 300.

(2) In response to an operation by the receiver B, the exponentiation unit 202, modular calculation unit 203 and calculation unit 204 of the receiver side apparatus 200 calculate, from the received ciphertext and by using the secret information, α'_1, α'_2, m' ($\alpha'_1 \in X_1$, $\alpha'_2 \in X_2$, $m' \in M$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = e/{u_1}^z$$

If the following is satisfied:

$${g_1}^{\alpha'_1}{u_1}^{x_1+\alpha' y_{11}+m' y_{21}}{u_2}^{x_2+\alpha' y_{12}+m' y_{22}} = v$$

m' is output as the deciphered results (where $\alpha' = \alpha'_1 \mid\mid \alpha'_2$), whereas if not satisfied, the effect that the received ciphertext is rejected is output as the decipher results.

With the scheme of this embodiment, it is possible to be semantically secure against adaptive chosen ciphertext attacks on the assumption of the Diffie-Hellman decision problem in G. The Diffie-Hellman decision problem is a problem of deciding whether a given sequence δ belongs to which one of the sets:

$$\mathbf{D} = \{(g_1, g_2, {g_1}^r, {g_2}^r) \mid r \in \mathbb{Z}_q\}, \quad \mathbf{R} = \{(g_1, g_2, {g_1}^{r_1}, {g_2}^{r_2}) \mid r_1, r_2 \in \mathbb{Z}_q,\ r_1 \neq r_2\}$$

relative to g_1, $g_2 \in G$:

If it is difficult to solve the Diffie-Hellman decision problem at a probability better than 1/2, it is said that the Diffie-Hellman decision problem is difficult (for the Diffie-Hellman decision problem, refer to the document 13 and the like).

The procedure of verifying security shows that if an algorithm capable of attacking the embodiment method exists, by using this algorithm (specifically, by the method similar to the method described in the document 12), an algorithm for solving the Diffie-Hellman decision problem can be configured.

Even if the algorithm for solving the Diffie-Hellman decision problem exists, since an algorithm capable of attacking the embodiment method is not still found, attacking the embodiment method is more difficult than solving at least the Diffie-Hellman decision problem.

With the embodiment method, when a ciphertext is generated in response to an operation by the sender A, the sender side apparatus 100 selects beforehand the random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$ and $r \in Zq$ and calculates and stores beforehand:

$$u_1 = g_1{}^r, \quad u_2 = g_2{}^r, \quad h^r, \quad g_1{}^{\alpha_1} c^r d_1{}^{\alpha r}$$

Therefore, a load of an encipher process can be reduced considerably and the process time can be shortened.

II Second Embodiment

The second embodiment shows one of the methods of realizing the public-key cryptographic scheme of the fist embodiment, and adopts concatenation of three parameters as a function π. Fig. 4 shows the outline of this embodiment.

1. Key Generation Process

In response to an operation by the receiver B, the key generator unit 201 of the reception side apparatus 200 generates beforehand secret information:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and public information:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1{}^{x_1} g_2{}^{x_2} \bmod p, \; d_1 = g_1{}^{y_{11}} g_2{}^{y_{12}} \bmod p, \; d_2 = g_1{}^{y_{21}} g_2{}^{y_{22}} \bmod p, \; h = g_1{}^z \bmod p,$
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q, \; 10^{k_3} < q, \; 10^{k_1+k_2+k_3} < p)$

(ord() indicates an order)

The public information is supplied to the sender side apparatus 100 or made public, via the communication line 300 or the like. A publicizing method may be registration in the third party (public information management facilities) or may be a well-known method.

Other information is stored in the memory unit 205.

2. Encipher/Decipher Process

(1) In response to an operation by the sender A, the random number generator unit 101 of the sender side apparatus 100 selects random numbers $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for a plaintext m ($|m| = k_3$, where $|x|$ indicates the number of digits of x) (step 401), and calculates (Step 402):

$$\tilde{m} = \alpha || m$$

The random number generator unit 101 further selects a random number $r \in Zq$, and the exponentiation unit 102, calculation unit 103 and modular calculation unit 104 calculates:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad e = \tilde{m}\, h^r \bmod p, \quad v = g_1{}^{\alpha_1} c^r d_1{}^{\alpha r} d_2{}^{mr} \bmod p$$

In response to an operation by the sender A, the communication apparatus 106 of the sender side apparatus 100 transmits (u_1, u_2, e, v) as the ciphertext to the receiver side apparatus 200 of the receiver B via the communication line 300 (Step 403).

(2) In response to an operation by the receiver B, the exponentiation unit 202, modular calculation unit 203 and calculation unit 204 of the receiver side apparatus 200 calculate (Step 404), from the received ciphertext and by using the secret information, α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|m'| = k_3$) which satisfy:

$$\alpha'_1||\alpha'_2||m' = e/u_1{}^z \bmod p$$

If the following is satisfied (Step 405):

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+m' y_{21}} u_2{}^{x_2+\alpha' y_{12}+m' y_{22}} \equiv v \pmod p$$

m' is output as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$) (Step 406), whereas if not satisfied, the effect that the received ciphertext is rejected is output as the decipher results (Step 407).

With the embodiment method, when a ciphertext is generated in response to an operation by the sender A, the sender side apparatus 100 selects beforehand the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) and $r \in Zq$ and calculates and stores beforehand:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad h^r \bmod p, \quad g_1{}^{\alpha_1} c^r d_1{}^{\alpha r} \bmod p$$

Therefore, a load of an encipher process can be reduced considerably.

III Third Embodiment

In this embodiment, the message sender A enciphers transmission data m to the receiver B by common-key encipher (symmetric cryptography), and the common key used is enciphered by the public-key cryptographic scheme of the first embodiment to be sent to the receiver B.

1. Key Generating Process

In response to an operation by the receiver B, the key generator unit 201 of the reception side apparatus 200 generates beforehand secret information:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and public information:

- G, G' : finite (multiplicative) group $\quad G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = {g_1}^{x_1} {g_2}^{x_2},\ d_1 = {g_1}^{y_{11}} {g_2}^{y_{12}},\ d_2 = {g_1}^{y_{21}} {g_2}^{y_{22}},\ h = {g_1}^{z},$
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- E : symmetric encipher function

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1,\ \forall \alpha_2 \in X_2)$$

M is a key space. The public information is supplied to the sender side apparatus 100 or made public, via the communication line 300 or the like. A publicizing method may be registration in the third party (public information management facilities) or may be a well-known method. Other information is stored in the memory unit 205.

2. Encipher/Decipher Process

(1) In response to an operation by the sender A, the random number generator unit 101 of the sender side apparatus 100 selects random numbers $\alpha_1 \in X_1$,

$\alpha_2 \in X_2$, $r \in Zq$ for the plaintext m ($m \in M$), and the exponentiation unit 102, calculation unit 103 and modular calculation unit 104 calculate:

$$u_1 = g_1{}^r, \quad u_2 = g_2{}^r, \quad e = \pi(\alpha_1, \alpha_2, K)h^r, \quad v = g_1{}^{\alpha_1} c^r d_1{}^{\alpha r} d_2{}^{Kr}$$

where $\alpha = \alpha_1 \mid\mid \alpha_2$. A ciphertext C of the transmission data m is generated by:

$$C = E_K(m)$$

by using the symmetric cryptographic function E and key data K. In response to an operation by the sender A, the communication apparatus 106 of the sender side apparatus 100 transmits (u_1, u_2, e, v, C) as the ciphertext to the receiver side apparatus 200 via the communication line 300.

(2) In response to an operation by the receiver B, the exponentiation unit 202, modular calculation unit 203 and calculation unit 204 of the receiver side apparatus 200 calculate, from the received ciphertext and by using the secret information, α'_1, α'_2, K' ($\alpha'_1 \in X_1$, $\alpha'_2 \in X_2$, $K' \in M$) which satisfy:

$$\pi(\alpha'_1 || \alpha'_2 || K') = e / u_1{}^z$$

If the following is satisfied (where $\alpha' = \alpha'_1 \mid\mid \alpha'_2$):

$$g_1{}^{\alpha'_1} u_1{}^{x_1 + \alpha' y_{11} + K' y_{21}} u_2{}^{x_2 + \alpha' y_{12} + K' y_{22}} = v$$

a decipher process is executed by:

$$m = D_{K'}(C)$$

where D is a decipher function corresponding to E. The deciphered results are output. If not satisfied, the effect that the received ciphertext is rejected is output as the decipher results.

As another method of generating a ciphertext C, the sender generates the ciphertext C by:

$$C = E_K(\alpha_1||\alpha_2||m)$$

by using the (symmetric) cryptographic function E and key data K. The receiver checks whether the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+K' y_{21}} u_2{}^{x_2+\alpha' y_{12}+K' y_{22}} = v,$$
$$\alpha'_1||\alpha'_2 = [D_{K'}(C)]^{k_1+k_2}$$

where $[x]^k$ indicates the upper k digits. If the check passes, a decipher process is executed by:

$$m = [D_{K'}(C)]^{-(k_1+k_2)}$$

where $[x]^{-k}$ indicates an integer train of x removed with the upper k digits.

With the embodiment method, when a ciphertext is generated in response to an operation by the sender A, the sender side apparatus 100 selects beforehand the random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$ and $r \in Zq$ and calculates and stores beforehand:

$$u_1 = g_1{}^r, \quad u_2 = g_2{}^r, \quad h^r, \quad g_1{}^{\alpha_1} c^r d_1{}^{\alpha r}$$

Therefore, a load of an encipher process can be reduced considerably and the .process time can be shortened.

IV Forth Embodiment

In this embodiment, the message sender A enciphers transmission data m to the receiver B by common-key encipher (symmetric cryptography), and the common key used is enciphered by the public-key cryptographic scheme of the second embodiment to be sent to the receiver B.

Fig. 5 shows the outline of the embodiment.

1. Key Generating Process

In response to an operation by the receiver B, the key generator unit 201 of the reception side apparatus 200 generates beforehand secret information:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and public information:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1{}^{x_1} g_2{}^{x_2} \bmod p,\ d_1 = g_1{}^{y_{11}} g_2{}^{y_{12}} \bmod p,\ d_2 = g_1{}^{y_{21}} g_2{}^{y_{22}} \bmod p,\ h = g_1{}^z \bmod p,$
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$
- E : symmetric encipher function

The public information is supplied to the sender side apparatus 100 or made public, via the communication line 300 or the like. A publicizing method may be registration in the third party (public information management facilities) or may be a well-known method. Other information is stored in the memory unit 205.

2. Encipher/Decipher Process

(1) In response to an operation by the sender A, the random number generator unit 101 of the sender side apparatus 100 selects random numbers $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for the key data K (Step 501) ($|K| = k_3$ where $|x|$ indicates the number of digits of x), and calculates (Step 502):

$$\tilde{\mathrm{m}} = \alpha || K$$

The random number generator unit 101 selects a random number $r \in Zq$, and the exponentiation unit 102, calculation unit 103 and modular calculation unit 104 calculate:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad e = \tilde{\mathrm{m}}\, h^r \bmod p, \quad v = g_1{}^{\alpha_1} c^r d_1{}^{\alpha r} d_2{}^{mr} \bmod p$$

In response to an operation by the sender A, the sender side apparatus 100 generates a ciphertext C of the transmission data m by:

$$C = E_K(m)$$

by using the (symmetric) cryptographic function E and key data K (Step 503), and the communication unit 106 transmits (u_1, u_2, e, v, C) as the ciphertext to the receiver side apparatus 200 via the communication line 300 (Step 504).

(2) In response to an operation by the receiver B, the exponentiation unit 202, modular calculation unit 203 and calculation unit 204 of the receiver side apparatus 200 calculate (Step 505), from the received ciphertext and by using the secret information, α'_1, α'_2, K' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|K'| = k_3$) which satisfy:

$$\alpha'_1||\alpha'_2||K' = e/{u_1}^z \bmod p$$

If the following is satisfied (where $\alpha' = \alpha'_1 \,||\, \alpha'_2$) (Step 506):

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+K' y_{21}} u_2{}^{x_2+\alpha' y_{12}+K' y_{22}} \equiv v \pmod p$$

a decipher process is executed (Step 507) by:

$$m = D_{K'}(C)$$

where D is a decipher function corresponding to E. The deciphered results are output. If not satisfied, the effect that the received ciphertext is rejected is output as the decipher results (Step 508).

As another method of generating a ciphertext C, the sender generates the ciphertext C by:

$$C = E_K(\alpha_1||\alpha_2||K)$$

by using the (symmetric) cryptographic function E and key data K. The receiver checks whether the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_{11}+K' y_{21}} u_2^{x_2+\alpha' y_{12}+K' y_{22}} \equiv v \pmod{p},$$
$$\alpha'_1 || \alpha'_2 = [D_{K'}(C)]^{k_1+k_2}$$

If the check passes, a decipher process is executed by:

$$m = [D_{K'}(C)]^{-(k_1+k_2)}$$

where $[x]^{-k}$ indicates an integer train of x removed with the upper k digits.

With the embodiment method, when a ciphertext is generated in response to an operation by the sender A, the sender side apparatus 100 selects beforehand the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$), $r \in Zq$ and calculates and stores beforehand:

$$u_1 = g_1^{r} \bmod p, \quad u_2 = g_2^{r} \bmod p, \quad h^{r} \bmod p, \quad g_1^{\alpha_1} c^{r} d_1^{\alpha r} \bmod p$$

Therefore, a load of an encipher process can be reduced considerably.

V Fifth Embodiment

In this embodiment, the message sender A transmits transmission data m to the receiver B by cryptographic communications by using symmetric cryptography based upon the public-key cryptography of the first embodiment. This embodiment is more excellent in the efficiency than the method of the third embodiment. If the symmetric cryptography is non-malleable (IND-CPA) against chosen plaintext attacks, it is possible to verify that the symmetric cryptography is non-malleable against adaptive chosen ciphertext attacks (NM-CCA2). In the embodiment method, a key K itself is not transmitted but the sender and receiver share a seed so that the key can be generated.

1. Key Generating Process

In response to an operation by the receiver B, the key generator unit 201 of the reception side apparatus 200 generates beforehand secret information:

- $x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$

and public information:

- G, G' : finite (multiplicative) group $\qquad G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = {g_1}^{x_1}{g_2}^{x_2},\ d = {g_1}^{y_1}{g_2}^{y_2},\ h = {g_1}^{z},$
- $\pi : X_1 \times X_2 \times M \longrightarrow \mathrm{Dom}(E)$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$ (Dom(E) is the domain of the function E)
- H : hash function
- E : symmetric encipher function

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1,\ \forall \alpha_2 \in X_2)$$

The public information is supplied to the sender side apparatus 100 or made public, via the communication line 300 or the like. A publicizing method may be registration in the third party (public information management facilities) or may be a well-known method. Other information is stored in the memory unit 205.

2. Encipher/Decipher Process

(1) In response to an operation by the sender A, the random number generator unit 101 of the sender side apparatus 100 selects random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Zq$ for transmission data m ($m \in M$, M is a plaintext space), and the exponentiation unit 102, calculation unit 103 and modular calculation unit 104 calculate:

$$u_1 = {g_1}^r, \quad u_2 = {g_2}^r, \quad v = {g_1}^{\alpha_1} c^r d^{\alpha r}, \quad K = H(h^r)$$

where $\alpha = \alpha_1 \;||\; \alpha_2$. A ciphertext C of the transmission data m is generated by:

$$C = E_K(\pi(\alpha_1, \alpha_2, m))$$

by using the (symmetric) cryptography. In response to an operation by the sender A, the communication apparatus 106 of the sender side apparatus 100 transmits (u_1, u_2, v, C) as the ciphertext to the receiver side apparatus 200 via the communication line 300.

(2) In response to an operation by the receiver B, the exponentiation unit 202, modular calculation unit 203 and calculation unit 204 of the receiver side apparatus 200 calculate:

$$K' = H({u_1}^z)$$

by using the secret information, and further calculate, from the received ciphertext, α'_1, α'_2 ($\alpha'_1 \in X_1$, $\alpha'_2 \in$

X_2) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = D_{K'}(C)$$

where D is a cryptographic function corresponding to E. If the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} = v,$$

m' is output as the deciphered results (where $\alpha' = \alpha'_1 \| \alpha'_2$), whereas if not satisfied, the effect that the received ciphertext is rejected is output as the decipher results.

With the embodiment method, when a ciphertext is generated in response to an operation by the sender A, the sender side apparatus 100 selects beforehand the random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$ and $r \in Zq$ and calculates and stores beforehand u_1, u_2 and v. Therefore, a load of an encipher process can be reduced considerably and the process time can be shortened.

VI Sixth Embodiment

In this embodiment, the message sender A transmits transmission data m to the receiver B by cryptographic communications by using symmetric cryptography based upon the public-key cryptography of the second embodiment.

Fig. 6 illustrates the outline of the embodiment.

1. Key Generating Process

In response to an operation by the receiver B, the key generator unit 201 of the reception side apparatus 200 generates beforehand secret information:

- $x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$.

and public information:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p,\ d = g_1^{y_1} g_2^{y_2} \bmod p,\ h = g_1^{z} \bmod p,$
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$
- H : hash function
- E : symmetric encipher function (the domain of E is all positive integers)

The public information is supplied to the sender side apparatus 100 or made public, via the communication line 300 or the like. A publicizing method may be registration in the third party (public information management facilities) or may be a well-known method. Other information is stored in the memory unit 205.

2. Encipher/Decipher Process

In response to an operation by the sender A, the random number generator unit 101 of the sender side apparatus 100 selects (step 602) random numbers $\alpha = \alpha_1 \| \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where $|x|$ is the number of digits of x) for the plaintext m (m∈M, M is a plaintext space) (Step 601), and further selects a random number r∈Zq. The exponentiation unit 102, calculation unit 103 and modular calculation unit 104 calculate:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad v = g_1{}^{\alpha_1} c^r d^{\alpha r} \bmod p, \quad K = H(h^r \bmod p)$$

The sender side apparatus 100 generates a ciphertext C of the transmission data m by:

$$C = E_K(\alpha_1 || \alpha_2 || m)$$

by using the (symmetric) cryptographic function E (Step 603). The communication apparatus 106 transmits (u_1, u_2, v, C) as the ciphertext to the receiver side apparatus 200 via the communication line 300 (Step 604).

In response to an operation by the receiver B, the exponentiation unit 202, modular calculation unit 203 and calculation unit 204 of the receiver side apparatus 200 calculate:

$$K' = H(u_1{}^z \bmod p)$$

by using the secret information, and further calculate (Step 605), from the received ciphertext, α'_1, α'_2 ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$) which satisfy:

$$\alpha'_1 || \alpha'_2 || m' = D_{K'}(C)$$

If the following is satisfied (Step 606):

$$g_1{}^{\alpha'_1} u_1{}^{x_1 + \alpha' y_1} u_2{}^{x_2 + \alpha' y_2} \equiv v \pmod p$$

m' is output as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$) (Step 607), whereas if not satisfied, the effect that the received ciphertext is rejected is output as the decipher results (Step 608).

With the embodiment method, when a ciphertext is generated in response to an operation by the sender A, the sender side apparatus 100 selects beforehand the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) and r Zq, and calculates and stores beforehand u_1, u_2 and v. Therefore, a load of an encipher process can be reduced considerably and the process time can be shortened.

VII Seventh Embodiment

In this embodiment, the message sender A transmits transmission data m to the receiver B by cryptographic communications by using another asymmetric cryptography and the public-key cryptography of the first embodiment. In this embodiment, a weak asymmetric cryptography (NM-CPA) can be transformed into a non-malleable cryptography (NM-CCA2).

1. Key Generating Process

In response to an operation by the receiver B, the key generator unit 201 of the reception side apparatus 200 generates beforehand secret information:

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : (asymmetric) decipher key

and public information:

- G : finite (multiplicative) group
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = g_1{}^{x_1} g_2{}^{x_2}$, $d = g_1{}^{y_1} g_2{}^{y_2}$,
- $\pi : X_1 \times X_2 \times M \longrightarrow \mathrm{Dom}(E)$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$ (Dom(E) is the domain of the function E)
- $E_{pk}(\cdot)$: (asymmetric cryptography) encipher function

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

M is a plaintext space. The public information is supplied to the sender side apparatus 100 or made public, via the communication line 300 or the like. A publicizing method may be registration in the third party (public information management facilities) or may be a well-known method. Other information is stored in the memory unit 205.

2. Encipher/Decipher Process

In response to an operation by the sender A, the random number generator unit 101 of the sender side apparatus 100 selects random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Zq$, and the exponentiation unit 102, calculation unit 103 and modular calculation unit 104 calculate:

$$u_1 = g_1{}^r, \quad u_2 = g_2{}^r, \quad v = g_1{}^{\alpha_1} c^r d^{\alpha r}$$

where $\alpha = \alpha_1 \; || \; \alpha_2$. The sender side apparatus 100 generates a ciphertext C of the transmission data m by:

$$e = E_{pk}(\pi(\alpha_1, \alpha_2, m))$$

by using the (asymmetric) cryptographic function E_{pk}. In response to an operation by the sender A, the communication apparatus 106 transmits (u_1, u_2, e, v) as the ciphertext to the receiver side apparatus 200 via the communication line 300.

In response to an operation by the receiver B, the exponentiation unit 202, modular calculation unit 203 and calculation unit 204 of the receiver side apparatus 200 calculate, from the received ciphertext, α'_1, α'_2 and m' ($\alpha'_1 \in X_1$, $\alpha'_2 \in X_2$, and $m' \in M$) which satisfy::

$$\pi(\alpha'_1, \alpha'_2, m') = D_{sk}(e)$$

(where D_{sk} is a decipher function corresponding to E_{pk}) by using the secret information. If the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} = v$$

where:

$$\alpha' = \alpha'_1 || \alpha'_2$$

m' is output as the deciphered results, whereas if not satisfied, the effect that the received ciphertext is rejected is output as the decipher results. With the embodiment method, when a ciphertext is generated in response to an operation by the sender A, the sender side apparatus 100 selects beforehand the random numbers $\alpha'_1 \in X_1$, $\alpha'_2 \in X_2$, and $r \in Zq$ and calculates and stores beforehand u_1, u_2 and v. Therefore, a load of an encipher process can be reduced considerably and the process time can be shortened.

VIII Eighth Embodiment

In this embodiment, similar to the seventh embodiment, the message sender A transmits transmission data m to the receiver B by cryptographic communications by using the asymmetric cryptography based upon the public-key cryptography of the second embodiment.

1. Key Generating Process

In response to an operation by the receiver B, the key generator unit 201 of the reception side apparatus 200 generates beforehand secret information:

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : (asymmetric cryptography) decipher key

and public information:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1{}^{x_1} g_2{}^{x_2} \bmod p,\ d = g_1{}^{y_1} g_2{}^{y_2} \bmod p,$
- k_1, k_2 : positive constant $(10^{k_1+k_2} < q)$
- $E_{pk}(\cdot)$: (asymmetric cryptography) encipher function (the domain is all positive integers)

The public information is supplied to the sender side apparatus 100 or made public, via the communication line 300 or the like. A publicizing method may be registration in the third party (public information management facilities) or may be a well-known method. Other information is stored in the memory unit 205.

2. Encipher/Decipher Process

In response to an operation by the sender A, the random number generator unit 101 of the sender side apparatus 100 selects random numbers $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where $|x|$ is the number of digits of x), and further selects a random number $r \in Zq$. The exponentiation unit 102, calculation unit 103 and modular calculation unit 104 calculate:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad v = g_1{}^{\alpha_1} c^r d^{\alpha r} \bmod p$$

In response to an operation by the sender A, the sender side apparatus 100 generates a ciphertext C of the transmission data m (positive integer) by:

$$e = E_{pk}(\alpha_1 || \alpha_2 || m)$$

by using the (asymmetric) cryptographic function E. The communication apparatus 106 transmits (u_1, u_2, e, v) as the ciphertext to the receiver side apparatus 200 via the communication line 300.

In response to an operation by the receiver B, the exponentiation unit 202, modular calculation unit 203 and calculation unit 204 of the receiver side apparatus 200 calculate, from the received ciphertext and by using the secret information, α'_1, α'_2 and m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, m' is a positive integer) which satisfy::

$$\alpha'_1||\alpha'_2||m' = D_{sk}(e)$$

where D_{sk} is a decipher function corresponding to E_{pk}. If the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} \equiv v \pmod{p},$$

where:

$$\alpha' = \alpha'_1||\alpha'_2$$

m' is output as the deciphered results, whereas if not satisfied, the effect that the received ciphertext is rejected is output as the decipher results. With the embodiment method, when a ciphertext is generated in response to an operation by the sender A, the sender side apparatus 100 selects beforehand the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$), and $r \in Zq$ and calculates and stores beforehand u_1, u_2 and v. Therefore, a load of an encipher process can be reduced considerably.

In each of the embodiments described above, cryptographic communications are performed by using the apparatuses of the sender and receiver, which is a general system. Various systems may also be used.

For example, in an electronic shopping

system, a sender is a user, a sender side apparatus is a computer such as a personal computer, a receiver is a retail shop and its clerk, and a receiver side apparatus is an apparatus in the retail shop such as a computer, e.g., a personal computer in the shop. An order sheet of a commodity ordered by the user or a key generated when the order sheet is enciphered is enciphered by the embodiment method and transmitted to the apparatus of the retail shop.

In an email cryptographic system, each apparatus is a computer such as a personal computer, and a message of the sender or a key generated when the message is enciphered is enciphered by the embodiment method and transmitted of the receiver side computer.

Each embodiment is also applicable to various systems using conventional cryptographic techniques.

Various digitalized data (multimedia data) can be used as a plaintext or message of each embodiment. Calculations of each embodiment are performed by executing each program in a memory by a CPU. Some of calculations may be performed not by a program but by a hardware calculation unit which transfers data to and from another calculation unit and CPU.